Homework 3

Mark Schulist

1)

1.a)

$$e : \mathbb{Z} \to \mathbb{Z}$$
$$e(n) = 2n + 1$$

Injective:

Proof:

$$a, b \in \mathbb{Z}$$
$$e(a) = e(b)$$
$$2a + 1 = 2b + 1$$
$$2a = 2b$$
$$a = b$$

We have shown that for any two values $a, b \in \mathbb{Z}$, in order for them to map to the same output they must be equal. Therefore, e is injective. $\square$

Not Surjective:

Proof: $0 \in \mathbb{Z}$, but there does not exist a value $a \in \mathbb{Z}$ such that $e(a) = 0$.

$$e(a) = 0$$
$$2a + 1 = 0$$
$$2a = -1$$
$$a = -\frac{1}{2}$$

$a \notin \mathbb{Z}$, so we have shown that there is a value in the cod(e) that e does not map a value from dom(e) to. $\square$

1.b)

$$f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$$
$$f(n) = (2n, n + 3)$$

Injective:

Proof:

$$a, b \in \mathbb{Z}$$
$$f(a) = f(b)$$
$$(2a, a + 3) = (2b, b + 3)$$

We can show that if the first component equals the other first component and the second component equals the other second component, then the two sides are equal.

$$2a = 2b$$
$$a = b$$

$$a + 3 = b + 3$$
$$a = b$$

The two sides are equal, therefore for any $a, b \in \mathbb{Z}$ we are will only get the same output if the two inputs are equal. $\square$

Not surjective:

Proof: $(0, 0) \in \mathbb{Z}^2$ but there does not exist an $a \in \mathbb{Z}$ such that $f(a) = (0, 0)$.

$$2n = 0$$
$$n = 0$$

But $f(0) = (0, 3)$ which is not $(0, 0)$. $\square$

1.c)

$$g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$g(m, n) = 3n - 4m$$

Not injective:

Proof:

$$g(3, 4) = 12 - 12 = 0$$
$$g(0, 0) = 0$$

We have shown that there are 2 inputs $\{(0, 0), (3, 4)\}$ that get mapped to the same value ($0 \in \mathbb{Z}$).

$\square$

Surjective:

Proof:

$$g(2, 3) = 9 - 8 = 1$$

We want to show that there exists a value $(a, b) \in \mathbb{Z}^2$ such that $g(a, b)$ can equal any value in $\mathbb{Z}$.

$$c \in \mathbb{Z}$$
$$g(2c, 3c) = c$$
$$9c - 8c = c$$

$\square$

1.d)

$$h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$h(m, n) = 2n - 4m$$

Not injective:

Proof:

$$h(0,0) = 0$$
$$h(1,2) = 0$$

We have shown that two different inputs map to the same value in h. □

Not surjective:

Proof: There does not exist $(a,b) \in \mathbb{Z}^2$ such that $h(a,b) = 1$.

$$h(a,b) = 1$$
$$2b - 4a = 1$$
$$b - 2a = \frac{1}{2}$$

It is not possible for the sum (or difference) of two integers to equal $\frac{1}{2}$. b is an integer and $2a$ is also an integer. □

1.e)

$$i : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$$
$$i(m,n) = (m+n, 2m+n)$$

Injective:

Proof: To prove i is injective, we must show that any two inputs $(a,b), (c,d) \in \mathbb{Z}^2$ must output the same value if and only if $(a,b) = (c,d)$.

$$i(a,b) = i(c,d)$$
$$(a+b, 2a+b) = (c+d, 2c+d)$$
$$a+b = c+d \qquad 2a+b = 2c+d$$
$$a-c = d-b \qquad 2a-2c = d-b$$
$$2(a-c) = d-b$$
$$2(d-b) = d-b$$
$$2d-2b = d-b$$
$$d = b$$
$$a-c = 0$$
$$a = c$$

We have shown that $a = c$ and $d = b$, which is the same as $(a,b) = (c,d)$. □

Surjective:

Proof: We want to show that we can get to any value $(a,b) \in \mathbb{Z}^2$ with i.

$$
\begin{aligned}
& i(m,n) = (a,b) \\
& a = m + n \qquad\qquad b = 2m + n \\
& n = a - m \\
& \qquad\qquad\qquad\quad b = 2m + a - m \\
& \qquad\qquad\qquad\qquad\quad b = m + a \\
& \qquad\qquad\qquad\qquad\quad m = b - a \\
& n = a - b + a \\
& n = 2a - b
\end{aligned}
$$

We can get to any value $(a,b) \in \mathbb{Z}^2$ using the equations above for n and m.

For example, if we want to get to $(4,5)$, we can do the following:

$$i(b-a, 2a-b)$$
$$i(5-4, 8-5)$$
$$i(1,3) = (4,5)$$

□

i is injective and surjective $\implies i$ is bijective.

2)

$$f : A \to B$$
$$g : B \to C$$

Given: $g \circ f$ is bijective.

Want to show: $g \circ f$ is bijective $\Rightarrow f$ is injective, g is surjective.

Proof: We can prove the contrapositive:

$$f \text{ not injective OR } g \text{ not surjective} \Rightarrow g \circ f \text{ not bijective}$$

Prove that f not injective $\Rightarrow g \circ f$ not bijective:

Suppose f not injective, then $\exists a_1, a_2 \in A$ distinct such that $g(f(a_1)) = g(f(a_2))$.

Prove that g is not surjective $\Rightarrow g \circ f$ not bijective:

$$\exists c \in C \text{ such that } \nexists g(b) = c \text{ and } \nexists g(f(a)) = c \in C$$

In other words, if g is not surjective, then we cannot “hit” every element $c \in C$, which is required for $g \circ f$ to be bijective. □

3)

$$f : A \to B$$
$$g : B \to C$$
$$h : B \to C$$

3.a)

Given: f is surjective and $g \circ f = h \circ f$

Want to show that $g = h$.

Proof: Because f is surjective, $\forall a \in A, \exists b \in B$ such that $f(a) = b$. Therefore, g and h must map every element $b \in B$ to the same element $c \in C$ because $g \circ f = h \circ f$.

In symbols, if $f(a) = b \forall b \in B \Rightarrow g(b) = h(b) \Rightarrow g(f(a)) = h(f(a))$.

If an element $b \in B$ was mapped to different elements by h and g, it is not possible for $g \circ f = h \circ f$ because $g(f(a)) \neq h(f(a))$. □

3.b)

$$f : \mathbb{N} \to \mathbb{N}$$
$$f(n) = 2n - 1$$
$$g : \mathbb{N} \to \mathbb{N}$$
$$g(n) = n$$
$$h : \mathbb{N} \to \mathbb{N}$$
$$h(n) = \begin{cases} n \text{ if } n \text{ is odd} \\ 2 \text{ if } n \text{ is even} \end{cases}$$

f only outputs odd values, so we can send all of the even values to wherever and still have $g \circ f = h \circ f$.

4)

4.a)

$$S : \mathcal{F}(A, \{0, 1\}) \to \mathcal{P}(A)$$

Proof: We can define $S(f) = \{a \in A | f(a) = 1\}$. In this case, $A = \text{domain}(f)$. We know the following is true by the definition of $\mathcal{F}(A, \{0, 1\})$:

$$f : A \to \{0, 1\}$$

We can show that S is injective. Two functions of the form $(f : A \to \{0, 1\})$ are unique if they map at least one input to a different output. When applied to our function declaration f, two different functions (let's say g and g') are distinct if $\{a \in A \mid g(a) = 1\} \neq \{a \in A \mid g'(a) = 1\}$. That is exactly what our function S does, meaning that the only way for $S(h) = S(h')$ is when $h = h'$.

We can also show that S is surjective. Given a set A (the same set as used above) and a set $B \subseteq A$, we can construct a function F that will return a function $f \in \mathcal{F}(A, \{0, 1\})$.

$$F : \mathcal{P}(A) \to \mathcal{F}(A, \{0, 1\})$$
$$F(X) = \begin{cases} 1 \text{ if } a \in X \\ 0 \text{ if } a \notin X \end{cases}$$

This function is the inverse of S, showing that S is surjective, and by extension, bijective. □

4.b)

We showed that there is a bijection between $\mathcal{F}(A, \{0, 1\})$ and $\mathcal{P}(A)$ so their cardinalities must be equal. We know $|\mathcal{P}(A)| = 2^{|A|}$, so the cardinality of $\mathcal{F}(A, \{0, 1\}) = 2^{|A|}$.

4.c)

The cardinality of $\mathcal{F}(A, B) = |B|^{|A|}$. Each $a \in A$ has $|B|$ possibilities to go to, so we end up with $|B| \cdot |B| \cdot |B| \cdot \ldots$, where there are $|A|$ $|B|$'s being multiplied together.

5)

5.a)

$$\{0, 1\} \times \mathbb{N} \to \mathbb{N}$$

We can map all of the elements in the codomain that have 0 as their first term to the even numbers, and all of the elements that have 1 as their first term to the odd numbers.

$$f(n) = \begin{cases} 2n \text{ if first term is 0} \\ 2n - 1 \text{ if first term is 1} \end{cases}$$

5.b)

$$\{0, 1\} \times \mathbb{N} \to \mathbb{Z}$$

We can do something similar, but we need to be careful because $0 \notin \mathbb{N}$.

$$g(n) = \begin{cases} n \text{ if first term is 0} \\ 1 - n \text{ if first term is 1} \end{cases}$$